

REMARKS/ARGUMENTS

Claims 1, 3, 20, 25 and 28-31 are pending in this application. By this Amendment, claims 1, 3, 20 and 25 are amended, claims 28-31 are added, and claims 2, 4-16, 18, 19, 22-24, 26 and 27 are canceled without prejudice or disclaimer. Support for the claims can be found throughout the specification, including the original claims and the drawings. Withdrawal of the rejections in view of the above amendments and the following remarks is respectfully requested.

I. Rejections Under 35 U.S.C. §103(a)

The Office Action rejects claims 1, 2, 4, 5, 7, 9, 10, 21 and 25-27 under 35 U.S.C. §103(a) over He in view of Bonnaure, and in further view of Eide. Claim 21 was cancelled in the Amendment filed on December 10, 2007, and claims 2, 4, 5, 7, 9, 10, 26 and 27 have been cancelled by this Amendment. The rejection, in so far as it applies to claims 1 and 25, is respectfully traversed.

Independent claim 1 is directed to a method for receiving information from an information service provider using an Internet TV. Independent claim 1 recites that the method includes (a) transmitting an authentication request message to an information provider server requesting authentication for receiving information during a first session, (b) receiving a message from the server requesting an authentication number, and (c) if the authentication number is available in a memory device of the Internet TV, transmitting the authentication number to the information provider server so that the information provider server checks validity of the authentication number. Independent claim 1 also recites that the method includes (d) if the

authentication number is not available in the memory device, registering a user with the information provider server, and receiving a new authentication number to store in the memory device, (e) receiving information from the information provider server and logging out to complete the first session, and (f) transmitting the authentication request message to the information provider server requesting authorization for a second session, and, in response to a request from the information provider server, transmitting the authentication number stored in the memory device to the information provider server so that the information provider server checks the validity of the authentication number, and receiving information from the information provider server during the second session.

He neither discloses nor suggests such features, or the claimed combination of features.

He discloses a system in which an authentication server 202 validates a user registration (S406), and a credential server 204 checks precision of the user's credentials (S408). These results are screened (S410), and information flows between accessible network elements 102 and the user (S412). To perform an initial login, the user enters an ID and password (S602), the ID and password are authenticated (S604), and an access list is constructed for the user (S608). A general ticket is issued to allow access to the network elements 102 in the access list (S610, S612), and a session ticket and a session encryption key is issued to allow access to a selected element 102 during that session (S706, S708). Upon logging out, the general ticket, the session ticket, and the session encryption key are destroyed, and the process must be repeated for access during a later session.

The Office Action asserts that He discloses establishing multiple sessions with different network elements using the same general ticket during a single log-on. Independent claim 1 recites a step (f) in which the same authentication number is actually used to initiate a second session. In this context, it would be well understood by one of ordinary skill in the art that the term 'second session' does not include probable connections to different network elements, but rather refers to a condition in which the Internet TV is connected to the same server. Further, the authentication number stored in the memory device is used to automatically establish the second session after the first session is completed upon logging-out. In contrast, in He's system, the general ticket, the session ticket, and the session encryption key are destroyed upon logging out, and authentication using ID and password input by the user must be repeated for logging in the system. Thus, He neither discloses nor suggests all of the steps recited in independent claim 1.

Further, Bonnaure is merely cited as allegedly teaching an Internet TV, and for at least this reason fails to overcome the deficiencies of He. Further, Bonnaure discloses a routing system for routing an Internet access request among a variety of on-line service providers based on geographic information of the client. Bonnaure's system routes the access request from the client such that the client accesses the network through a point of presence node closest to the client so as to incur minimum cost. Bonnaure's disclosure is directed mainly to accessing Internet subscriber networks at minimum cost. Bonnaure is essentially silent as to any type of authentication process in accessing the contents provided a service provider.

Further, Eide is merely cited as allegedly teaching an identification number comprising a model name or manufacturing date, and for at least this reason fails to overcome the deficiencies of He and Bonnaure.

Accordingly, it is respectfully submitted that independent claim 1 is allowable over the applied combination, and thus the rejection of independent claim 1 under 35 U.S.C. §103(a) over He, Bonnaure and Eide should be withdrawn. Dependent claim 25 is allowable over He, Bonnaure and Eide at least for the reasons set forth above with respect to independent claim 1, from which it depends, as well as for its added features.

The Office Action rejects claims 1-4, 7-10, 14, 20 and 22-27 under 35 U.S.C. §103(a) over Bonnaure in view of Nobakht. Claims 2, 4, 7-10, 14, 22-24, 26 and 27 have been cancelled by this Amendment. The rejection, in so far as it applies to claims 1, 3, 20 and 25, is respectfully traversed.

The features of independent claim 1 are set forth above. As also set forth above, Bonnaure neither discloses nor suggests all of the features of independent claim 1. Further, Nobakht fails to overcome the deficiencies of Bonnaure.

Bonnaure discloses an execution process in FIGS. 7-15, a process for brokering real-time network game in FIG. 16 using the execution process shown in FIGS. 7-15, and a routing process for achieving minimum cost on-line access in FIGS. 17 and 18 using the execution process shown in FIGS. 7-15.

In the system shown in FIGS. 7-15 of Bonnaure, a WebTV server 620 provides

optimized routing service to a client 610. A private server 820, which is added to enhance communication security between the WebTV server 620 and the client 610, defines parameters for the client 610 through a secure channel before the client 610 is connected to the WebTV server 620. The client 610 accesses the private server 820 before accessing the WebTV server 620. The private server 820 detects the network address of the client 610 to provide to the client 610. If the client 610 does not have an encryption key, the private server 820 provides the client 610 with an encryption key. Further, the private server 820 provides the address of a point of presence node closest to the client 610. Subsequently, the client 610 terminates the connection with the private server 620 and opens a new connection to the WebTV server 620. The WebTV server 620 receives a client box identifier and the client network address from the client 610 to compare with those in the server, which the WebTV server obtains from the private server 820. If the information from the client 610 is identical to that in the server, the WebTV server 620 geographically optimizes the service request from the client 610. If there is any discrepancy between the information, however, the process is terminated.

FIG. 16 of Bonnaure provides a working example of the process shown in FIGS. 7-15, in which the WebTV server 620 intermediates a real-time network game between clients. After terminating the connection to the private server 620, the client 610 opens a connection to the WebTV server 620 and provides the WebTV server 620 with the client box identifier and the client network address. If the client 610 submits a request to match the client with another remote game player, the WebTV server 620 provides the client 610 with the network address of

a new remote client. After receiving the network address of the new remote client, the client 610 disconnects from the WebTV server 620 and establishes a direct communication link with the new remote client to initiate real-time game playing.

FIGS. 17 and 18 of Bonnaure are modified embodiments of the system shown in FIGS. 7-15. When a customer accesses a central access server 1724, the central access server 1724 identifies the customer using Automatic Number Identification (ANI), and generates and provides an algorithm for use by the customer to choose an Internet access provider according to customized criteria. The customer can execute the algorithm to choose a compatible Internet access provider, and access the Internet through the chosen access provider.

It appears the Office Action has drawn a comparison between the encryption key disclosed by Bonnaure and the claimed authentication number. However, as would be well understood by one of ordinary skill in the art, in this context, the term “authentication” would typically refer to the verification of the identity of a person. In contrast, the term “encryption” would typically refer to the process of encoding a message so that it can be read only by the sender and the intended recipient, as disclosed by Bonnaure (see column 12/lines 30-35 of Bonnaure). Thus, it is respectfully submitted that the encryption key disclosed by Bonnaure is not properly compared to the claimed authentication number, nor the process Bonnaure disclosed by Bonnaure which makes use of such an encryption key comparable to the claimed authentication process.

Additionally, even if such an improper comparison is drawn, in Bonnaure’s system, the

Reply to Office Action of March 3, 2009

client 610 first connects to the private server 820 to get the network address of the client and the encryption key for the client, and tries access to the WebTV server 620 only when the encryption key received from the private server 820 is assuredly stored in the client 610 (FIG. 11, steps 1112 and 1120). In contrast, in the method recited in independent claim 1, the Internet TV provides the authentication number to the server in response to the request from the server, and gets a new authentication number only when there is no authentication number in the memory device of the Internet TV. Thus, the new authentication number is only issued when an attempt was made to use an authentication number stored in the memory device of the Internet TV, but none was found. Therefore, even if Bonnaure's encryption key is improperly compared to the claimed authentication number, Bonnaure still neither discloses nor suggests the feature recited in step (d) of independent claim 1.

The Office Action asserts that, alternatively, the client box identifier or the client network address disclosed by Bonnaure may instead be compared to the claimed authentication number. Applicant respectfully disagrees. In the method recited in independent claim 1, the Internet TV may have the authentication number stored in its memory device, and may provide the authentication number to the server just after an authentication request message is transmitted to the server, so that the server checks validity of the authentication number. In contrast, in the system shown in FIGS. 7-15 of Bonnaure, the client 610 first accesses the private server 820 before accessing the WebTV server 620, and the private server 820 attempts to detect the client network address using ANI, generates the encryption key, and determines an appropriate point

of presence node. After the client 610 is disconnected from the private server 820 and connected to the WebTV server 620, the WebTV server 620 identifies the client using the client box identifier and the client network address received from the client.

Neither the WebTV server 620, the private server 820, nor the combination thereof performs the same process as that of the server recited in claim 1. That is, FIGS. 7-15 of Bonnaure and the accompanying description thereof neither discloses nor suggests performing a user registration process and generating an authentication number for storage in the memory only when there exists no authentication number in the memory device of the client, as recited in step (d) of independent claim 1. Further, FIGS. 7-15 of Bonnaure and the accompanying description thereof neither discloses nor suggests re-using such an authentication number in a second session being separately established after the first session is completed, as recited in step (f) of independent claim 1. Rather, in Bonnaure's system, the client box identifier always resides in the client 610 and never is updated, while the client network address is obtained from the private server 820 whenever the connection to the WebTV server 620 is carried out. Even in the process shown in FIGS. 17 and 18 of Bonnaure, the central access server 1724 identifies the customer using ANI, and does not directly receive any authentication information from the customer 1710, nor does it provide services in response to any such authentication information. Thus, FIGS. 17 and 18 and the accompanying description thereof neither discloses nor suggests the features as recited in steps (d) and (f) of independent claim 1.

Further, Nobakht is merely cited as allegedly teaching the use of model information and manufacturing date in an identification number, and for at least this reason fails to overcome the deficiencies of Bonnaure.

Accordingly, it is respectfully submitted that independent claim 1 is allowable over the applied combination, and thus the rejection of independent claim 1 under 35 U.S.C. §103(a) over Bonnaure and Nobakht should be withdrawn. Dependent claims 3, 20 and 25 are allowable at least for the reasons set forth above with respect to independent claim 1, from which they depend, as well as for their added features.

The Office Action rejects claims 5, 6, 11-13, 18 and 19 under 35 U.S.C. §103(a) over Bonnaure in view of Dorfman. Claims 5, 6, 11-13, 18 and 19 have been cancelled by this Amendment, and thus this rejection is moot.

II. New Claims 28-31

New claims 28-31 are added to the application. It is respectfully submitted that new claims 28-31 meet the requirements of 35 U.S.C. §112, and also define over the applied prior art.

More specifically, new independent claim 28 is directed to a method for receiving information from an information provider server, including (a) transmitting an authentication request message to the information provider server requesting authentication for receiving information, (b) receiving a message from the information provider server requesting an authentication number, (c) if the authentication number is available in a memory device of the Internet TV, automatically transmitting the authentication number to the information provider server so that the

information provider server checks validity of the authentication number, (d) if the authentication number is not available in the memory device, registering a user with the information provider server and receiving a new authentication number to store in the memory device, (e) receiving the information from the information provider server and logging out from the information provider server, and (f) transmitting the authentication request message to the information provider server, and automatically reading out the authentication number from the memory device to transmit to the information provider server so that the information provider server checks the validity of the authentication number, and receiving the information from the information provider server.

New independent claim 31 is directed to an Internet TV apparatus. New independent claim 31 recites, *inter alia*, that the Internet TV apparatus conducts an access procedure, comprising sending, to the server, an access request message, receiving, from the server, a request for an authentication number, sending, to the server, the requested authentication number retrieved from the memory, and receiving, from the server, information that is then decoded and displayed on the display screen if the authentication number results in successful authentication of the Internet TV apparatus. The Internet TV also conduces a re-access procedure, comprising sending, to the server, another access request message, receiving, from the server, another request for an authentication number, sending, to the server, the same authentication number previously used in the access procedure that resulted in successful authentication of the Internet TV apparatus, and receiving, from the server, information that is

then decoded and displayed on the display screen.

As set forth above, He, Bonnaure, Eide and Nobakht, either alone or in combination, neither disclose nor suggest the features of new independent claims 28 and 31, or the respective claimed combination of features. New dependent claims 29 and 30 are allowable at least for the reasons set forth above with respect to independent claim 28, from which they depend, as well as for their added features.

III. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned, **Joanna K. Mason**, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this,


Serial No. **09/996,718**

Docket No. **P-0303**

Reply to Office Action of **March 3, 2009**

concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
KED & ASSOCIATES, LLP

A handwritten signature in black ink, appearing to read 'Daniel Y.J. Kim', with a long horizontal flourish extending to the right.

Daniel Y.J. Kim
Registration No. 36,186

Joanna K. Mason
Registration No. 56,408

P.O. Box 221200
Chantilly, Virginia 20153-1200
703 766-3777 DYK:JKM:ldh

Date: May 27, 2009

Q:\Documents\2000-236\196210

Please direct all correspondence to Customer Number 34610